СИЛАБУС
Кафедра кібербезпеки та математичного моделювання

Назва курсу	Технології безпеки web-ресурсів
Мова викладання	українська
Викладач (-і)	Базилевич В.М., к.е.н., доцент, зав. кафедри інформаційних та комп'ютерних систем
Профайл викладача (-ів)	Web: https://cs.stu.cn.ua/ ResearcherID: G-5764-2014 ORCID: 0000-0001-8935-446X
Контакти викладача	bazvlamar@stu.cn.ua

1. Анотація курсу

Цей курс знайомить вас із кібербезпекою для хмари. Ми вивчимо та застосуємо класичні методи безпеки для сучасних проблем безпеки в хмарі. Ми проаналізуємо останні вразливості хмарної безпеки, використовуючи стандартні систематичні методи. Ми створимо наші власні приклади використання веб-сервісу та розробимо для них рішення безпеки.

Модуль 1. Змістовий модуль 1.

Тема 1. Вступ

Представлення безпеки Інтернет-сервера в шість кроків, детально виствітлення перших трьох. Крок 1: Ізольована служба настільних ПК. Крок 2. Підвищена міцність. Крок 3. Розподілені обов'язки.

Тема 2. Безпека мережі для приватної хмари

Методи контролю того, як різні хости взаємодіють у мережі. Крок 4. Додавання шкали. Мережева адресація. Шари мережевого протоколу. Мережеві пристрої. Контроль безпеки: фільтрація пакетів. Управління ланцюгами та вмістом. Концепція хмарних послуг для експертної оцінки.

Тема 3. Криптографія для віддаленого доступу та підтримки

Сучасні системи далеко не завжди працюють всередині однієї межі довіри. Ми будемо використовувати криптографію для захисту інформації, коли вона виходить за межі нашої довіри. Аутентифікація криптовалют. Аутентифікація сервера. Сертифікати відкритого ключа. Крок 5 Послуги. Використання CVSS для оцінки вразливості хмари.

Тема 4. Безпека хмари

Розгляд переваг та викликів публічної хмари. Ми будемо використовувати методи з попередніх тем для вирішення питань безпеки хмари. Хостинг публічної хмари. Розробка моделей безпеки. Архітектура хмарних сервісів. Віртуалізація комп'ютерних систем, процесів, мереж. Шари протоколів та криптографія. Планування безпеки архітектури хмари. Створення базового плану безпеки хмарного сервісу.

2. Мета курсу

Мета дисципліни – вивчити класичні прийоми безпеки для сьогоднішніх хмарних проблем безпеки. Забезпечення безпеки веб-сервісів та вирішення проблем, що виникають під час його вдосконалення. Проаналізувати останні вразливості хмарної безпеки, використовуючи стандартні, систематичні методи. Створення власних прикладів веб-служб та рішень безпеки для них.

Під час вивчення дисципліни здобувач вищої освіти (ЗВО) має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності 125 - Кібербезпека:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КФ 2. Здатність розробляти, впроваджувати і супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах (автоматизованих систем та їх додатків) та у інфраструктурі організації в цілому.

3. Результати навчання

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання, передбачені освітньою програмою:

ПРН 2. планувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

ПРН 3. використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН 7. проектувати, впроваджувати, та супроводжувати інформаційно-комунікаційні системи, а також забезпечувати захист інформаційних ресурсів мереж (мережева безпека) та всієї інфраструктури установи на базі сучасних моделей, методів і засобів передачі даних в комутативних або без комутативних каналах зв’язку, хмарного простору, протоколів обміну даними, мережного устаткування, тощо.

Завдання – навчитись проектувати та адмініструвати локальні обчислювальні мережі, використовуючи сучасні технології обміну даними.

В результаті вивчення навчальної дисципліни студент повинен

знати:

– останні вразливості хмарної безпеки;

– стандартні, систематичні методи захисту;

– класичні концепції безпеки, такі як найменший привілей та розподіл обов’язків, а також більш технічні криптографічні засоби та методи контролю доступу.

вміти:

- створювати та підтримувати простий хмарний сервіс;
- вставновлювати ролі для послуги;
- оцінювати ризики, закладені у вразливих ситуаціях;
- застосовувати основні методи захисту хмарних сервісів.

4. Обсяг курсу. Зазначте загальку кількість кредитів, кількість занять та годин самостійної роботи

Вид заняття	**Загальна к-сть годин**
лекції	16
лабораторні	14
самостійна робота (РГР)	90

5. Пререквізити - Передумови для вивчення дисципліни: для ефективного засвоєння матеріалів курсу «Технології безпеки web-ресурсів» доцільно попередньо вивчити такі курси: Основи криптографії, Комп'ютерні мережі, Інтернет-технології.

6. Система оцінювання та вимоги

Оцінювання проводиться за 100-бальною шкалою.

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 48% семестрової оцінки;
- тест: 12% семестрової оцінки;
- іспит: 40% семестрової оцінки.

Загальна система оцінювання курсу	
Лабораторні роботи	**Критерії оцінювання лабораторних робіт** 1. Підготовленість до лабораторних занять 2. Самостійність виконання лабораторних робіт. 3. Повнота розкриття теми. 4. Своєчасність виконання лабораторних робіт
Умови допуску до підсумкового контролю	Позитивна оцінка за всіма обов'язковими видами робіт (лабораторні роботи та РГР)

7. Політики курсу -

Політика щодо академічної доброчесності: Списування під час контрольних робіт заборонені (в т.ч. із використанням мобільних девайсів). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки лабораторних завдань.

Жодні форми порушення академічної доброчесності не толеруються. У випадку таких подій – реагування відповідно до Положення про академічну доброчесність студентів та науково-педагогічних працівників НУ «Чернігівська політехніка» та Методичних рекомендацій для закладів вищої освіти з підтримки принципів академічної доброчесності

Правила перезарахування кредитів у випадку мобільності, правила перескладання або відпрацювання пропущених занять тощо: відбувається згідно з Положення про організацію освітнього процесу в НУ «Чернігівська політехніка».

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (до -50% від можливої максимальної кількості балів за вид діяльності балів).

Перескладання модулів відбувається за наявності поважних причин (наприклад, лікарняний).

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, хвороба, працевлаштування, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням.

8. Рекомендована література

1. Таненбаум Э. Компьютерные сети. / Э. Таненбаум — СПб.: Питер, 2012. – 960с.
2. Thomas E. Cloud Computing Design Patterns / E. Thomas, C. Robert, N. Amin., 2015. – 592 с. – (Prentice Hall). – (The Prentice Hall Service Technology Series from Thomas Erl by Thomas Erl).
3. Ivan R. Bulletproof SSL and TLS: The Complete Guide to Deploying Secure Servers and Web Applications / Ristic Ivan., 2014. – 425 с. – (Feisty Duck Ltd). – (ISBN 1907117040).
4. Dave M. S. Virtualization Security: Protecting Virtualized Environments / Shackleford Dave M.., 2012. – 368 с. – (Sybex). – (ISBN 1118331516).
5. Shao Y. Z. Guide to Security Assurance for Cloud Computing / Y. Z. Shao, H. Richard, T. Marcello., 2016. – (Springer). – (ISBN 3319259865).
6. Chris D. Practical Cloud Security: A Guide for Secure Design and Deployment / Dotson Chris., 2019. – 196 с. – (O'Reilly Media). – (ISBN-13: 978-1492037514).

Інформаційні ресурси

1. https://www.coursera.org/learn/cloud-security-basics/home/welcome
2. https://www.redhat.com/en/topics/security/cloud-security
3. https://aws.amazon.com/security/
4. https://cloud.google.com/security